United States
Department of Agriculture

Office of the Chief Information Officer (OCIO)
Year 2000 Program Office

Year 2000 Business Continuity (Contingency) Planning Guide

Table of Contents

1.0 Introduction

The United States Department of Agriculture (USDA) faces a unique set of challenges as the Year 2000 approaches.

The challenge is unique in that its scope is major and its due date unalterable. The scope is pervasive and carries unusually high risks. USDA needs to identify all potential risks and threats to the continuity of its business, develop actions to mitigate those risks and contingency plans to continue business if failure occurs. The Year 2000 crisis can be viewed as a natural disaster of sorts. It won't be induced by acts of nature but rather by the calendar. As such it posses a significant threat to continuous business operations and should be treated in much the same way a natural disaster would be handled. Reviewing the disaster recovery plans in each Agency will provide a point of departure to assist in the development of detailed Business Continuity (Contingency) Plans and will provide an excellent opportunity for the simultaneous review of those plans. However, the focus must remain on developing plans that will safeguard an agency's ability to produce a *minimum acceptable level* of outputs and services in the event of failures of internal or external mission-critical information systems and services.

The Year 2000 challenge is Government-wide as well as global. Every Federal, State and local government department and every business within the private sector face similar risks. USDA customer base includes virtually every American citizen, legal aliens, and many foreign nationals living abroad which makes it incumbent for the Department to prepare and continue its business uninterrupted into the Year 2000.

Within the seven mission areas of USDA business operations, both at the Agency level and at the Field Operation level, there are multiple dependencies on computer systems and microchip technology to perform day-to-day functions.

Transitioning into the next millennium requires a review of all business processes to determine the impact the century date change will have on program delivery.

The potential impact extends beyond USDA's internal information systems. USDA depends on data provided by its business partners including other Federal agencies, States, third parties, and vendors who provide telecommunications, software and other goods and services. Also, USDA depends on services provided by the public infrastructure including power, water, transportation, and voice and data telecommunications. It is with these impacts in mind that has necessitated the Secretary to establish the following priorities for the Department:

- **Health and Safety Risk**: Adverse effect on the health and safety of USDA Customers, partners, or employees. This includes areas such as food safety, disease monitoring, and prevention of physical security and safety.

- **Financial Impact**: Adverse effect individual financial security. This includes food assistance, loan servicing or crop insurance.
- **Economic Repercussions**: Adverse effect on agriculture markets or trade. Examples include market news and data or commodities tracking.

1.1 Purpose

The purpose of this guide is to provide direction and outline for USDA agencies to identify, assess, manage, and mitigate Year 2000 risks to ensure the continuity of USDA core business processes. USDA Year 2000 *Business Continuity (Contingency) Plan* (BCP) will prepare the Department to avoid a crisis that could result if systems are unable to recognize Year 2000 dates. Resources critical to operating USDA's core business processes and key support processes, must be identified to provide a basic level of services until the normal level of services can be restored to all customers. The BCP identifies risks and threats, establishes mitigation strategies for the identified risks and threats; and provides contingencies in the event risk mitigation efforts fail.

USDA has a Year 2000 Program, with dedicated resources in place, to ensure that its automated systems function correctly beginning January 2000. USDA has taken every precaution to ensure it will complete all renovations of its systems by March 1999. Detailed procedures must be developed and implemented for formal certification of mission critical systems.

The certification, comprising baseline testing, simulated forward-date testing and forward-date integration testing if not already begun, must begin immediately. Post-implementation reviews will begin in the fall of 1998 and continue during 1999. Although these efforts greatly reduce the chance of a systems failure, there are no guarantees that automated systems will not be adversely affected. USDA has numerous data exchanges with external trading partners and also relies on external sources to provide basic services such as electric power and telecommunications. While USDA is working closely with external organizations and expects these systems and services to be available, the BCP will ensure that business processes can continue in the event of an unexpected failure.

1.2 Use and Scope

The successful operation of the Department's core business processes depends heavily on complex information systems, a wide range of internal and external products and services, and on the uninterrupted operations of the major information technology infrastructure. This guide should be used to develop a business continuity plan to ensure that Mission Area core business processes and key support processes remain the central focus in preparing automated systems for the Year 2000. The resulting high level plan identifies broad areas of risk and general mitigation strategies and contingencies.

For each core business process and key support process, risk mitigation strategies and contingency plans will work together to ensure those processes continue uninterrupted. As risk mitigation strategies are implemented, the degree of risk decreases and the likelihood of needing to implement the contingency plan is reduced.

The scope of the BCP guide is broad and comprehensive. It covers the enterprise-wide infrastructure that supports business operations at the national and local levels. From a business perspective, potential risks and threats must be identified along with risk-mitigation strategies for each Mission Area. Contingencies must also be provided in the event risks and threats are not successfully mitigated. An interruption in the infrastructure could affect USDA ability to provide services to its customers. This guide outlines the process methodology to use for identification of core business processes, and outlines the strategies to provide for the continuation of services. A glossary of terms is included at **Appendix A** to assist in understanding the contents in this guide.

1.3 Assumptions

This guide uses the following assumptions:

- USDA offices will be open for business on Monday, January 3, 2000;
- USDA will plan for business as usual in that all offices will be ready for the full range of business transactions; and
- In the event that unexpected failures occur, USDA Agencies will immediately implement their Business Continuity (Contingency) Plan to ensure that USDA's business processes continue.

1.4 Planning Process Methodology

The planning process methodology provides guidance in preparing a Business Continuity (Contingency) Plan for the Department. The focus is to centralize efforts within each Mission Area and Department Administration (DA) and Staff Offices. This will provide flexibility while ensuring that all Mission Areas receive the necessary support to develop the BCP.

The methodology complies with the guidelines established by GAO and reported in their Exposure Draft, titled "*Year 2000 Computing Crisis: Business Continuity and Contingency Planning*" dated March 1998. A sample template page from NFC, adapted from the Social Security Administration (SSA) plan, is included in **Appendix B**. The contingency plans developed with this methodology describe the steps USDA will take, to ensure the continuity of the core business processes in the event of a Year 2000-induced system failure.

All BCPs will be reviewed and approved by the Office of Chief Information Officer (OCIO) Year 2000 Program Office. All Mission Areas, the Departmental Administration, and Staff Offices must submit their Business Continuity Plan to the Office of the Chief Information Officer for final review and approval (see 1.4) for the Secretary.

2.0 Organization

2.1 Business Continuity Strategy

USDA's strategy for ensuring systems readiness for the Year 2000 centers on the core business processes and the key supporting processes. Planning for business continuity provides a prudent response to critical business risks that cannot be put to rest until all mission-dependent systems (telecommunications, information technology, and vulnerable systems and processes) have been shown to be operationally stable and free of Year 2000 problems.

USDA must analyze its core business processes to identify the risks or threats to providing uninterrupted service, and devise plans to activate should a failure occur. The risks and threats along with contingency planning measures are presented in *section 4* of the BCP.

2.2 Roles and Responsibilities

USDA's Office of the Chief Information Officer Year 2000 is responsible for providing leadership and oversight of the development of a comprehensive Year 2000 business continuity strategy. This strategy is focused on the Mission Area and the Agencies working together to develop a business continuity plan. To accomplish this activity, roles and responsibilities are defined as follows:

USDA Component	Component Contingency Planning Responsibility
Chief Information Officer	Provide overall Department-wide guidance on contingency planning and coordinate the development of the Departments BCP effort. Perform independent verification and validation of plans and review of all Mission Area BCPs for final approval on behalf of the Secretary.
Assistant and Under Secretaries for each	Coordinate and develop the Mission Area BCP. Provide assistance and resources to each Agency to

Mission Area	ensure that all agencies and operational elements have an approved BCP. Coordinate efforts with all external public and private organizations to ensure business continuity of services provided will continue with little or no disruption as a result of the Year 2000 problem for each Mission Area.
Agency Administrators and Senior Executive Sponsors	Develop business continuity and contingency plan for the Agency and all field operating organizations. Coordinate efforts with all external public and private organizations to ensure business continuity of services will continue with little or no disruption as a result of the Year 2000 problem.
Office of Communications	Develop business continuity and contingency plan for communicating to USDA customers and general public any matter of interest concerning Department operations affected by a Year 2000 contingency.

A diagram of these roles and responsibilities for the Mission Area and Agencies is shown in figure 2-1 below.

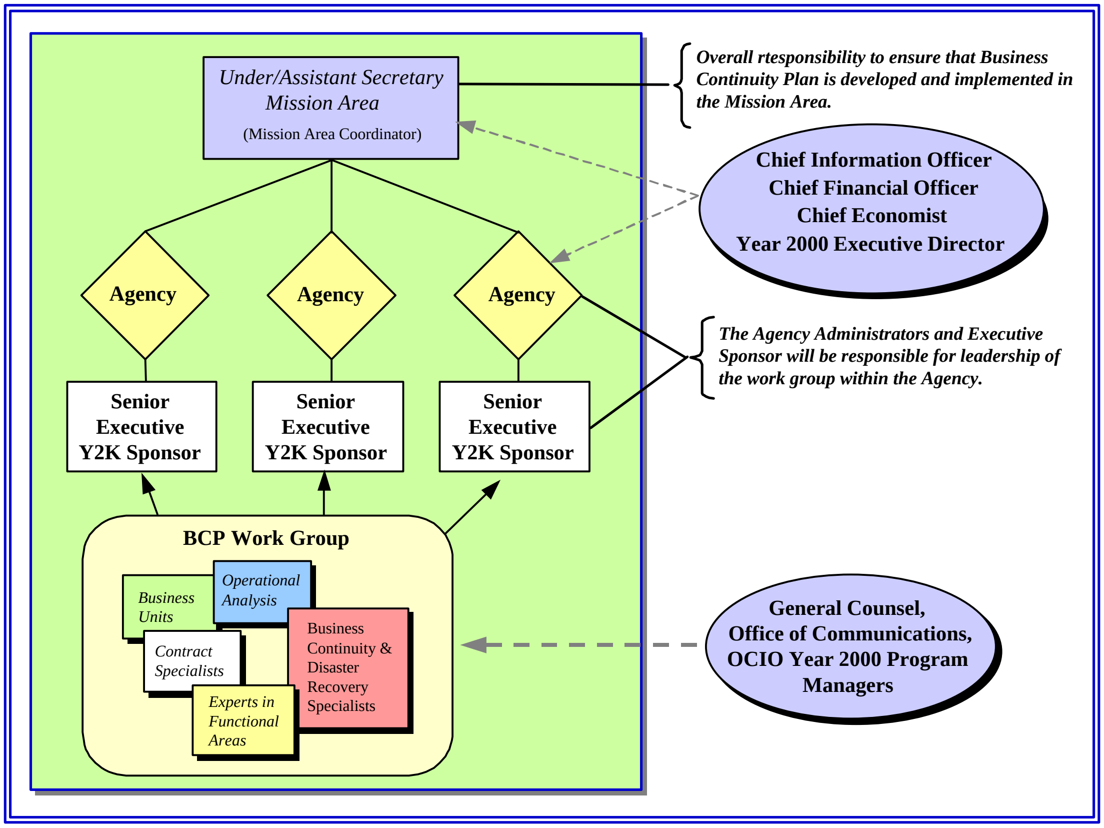

Under/Assistant Secretary
Mission Area
(Mission Area Coordinator)
Overall rtesponsibility to ensure that Business Continuity Plan is developed and implemented in the Mission Area.
Chief Information Officer
Chief Financial Officer
Chief Economist
Year 2000 Executive Director
Agency
Agency
Agency
The Agency Administrators and Executive Sponsor will be responsible for leadership of the work group within the Agency.
Senior Executive Y2K Sponsor
Senior Executive Y2K Sponsor
Senior Executive Y2K Sponsor
BCP Work Group
Business Units
Operational Analysis
Contract Specialists
Business Continuity & Disaster Recovery Specialists
Experts in Functional Areas
General Counsel,
Office of Communications,
OCIO Year 2000 Program Managers

Figure 2-1. *Business Continuity Planning Roles and Responsibilities*

2.3 USDA Core Business Processes

USDA core business processes depend on a complex technology infrastructure that is crucial for ongoing operations. Power, data, and voice telecommunications, along with the Department's computer operations hardware and software are essential to ensuring that USDA business processes continue uninterrupted. These automated systems are the means by which USDA is able to provide service on demand to the public, the Department's client population, other government entities, large and small corporations, and individual businesses.

2.4 Description of Mission Areas and Business Operations

The Department is organized into seven Mission Areas, Department Administration, Congressional Relations, and six Staff Offices. Each mission area is briefly described below.

2.4.1 Natural Resources and Environment

USDA plays a critical role in the sound stewardship of the Nation's land and natural resources. The Forest Service (FS) and the Natural Resources Conservation Service (NRCS) share responsibility for fostering sound stewardship on 75 percent of the country's total land area.

Both agencies apply sustainable ecosystem principles in the management of soil, water, forests, and wildlife. Each agency's respective strengths and expertise demonstrate that sound environmental policy and agricultural productivity are not mutually exclusive.

The FS provides leadership in the management protection, and use of the Nation's forests and rangelands. The agency is dedicated to multiple-use management of these lands for sustained yields of renewable resources such as wood, water, forage, wildlife, and recreation to meet the diverse needs of people.

The NRCS is the Federal agency that works hand-in-hand with the American people to conserve, improve, and sustain natural resources on private lands.

2.4.2 Farm and Foreign Agricultural Services

The Farm and Foreign Agricultural Services mission area is responsible for administering agricultural price and income support programs, production adjustment programs, and the Conservation Reserve Program. The Federal Crop Insurance Corporation programs are administered, as are the farm lending programs for agricultural producers and others engaged in production of agricultural commodities. Programs that support exports of agricultural products are administered including initiatives to combat unfair competition that develop new markets for U.S. suppliers, and that provide food assistance to food-deficit countries.

The Farm and Foreign Agricultural Services mission area is organized into three agencies, the Farm Services Agency, the Foreign Agricultural Service, and the Risk Management Agency

2.4.3 *Rural Development*

USDA has the unique responsibility of coordinating Federal assistance to rural areas of the Nation. The Rural Development mission is to help rural Americans improve the quality of their lives.

The Rural Development Mission Area is organized into three areas: the Rural Utilities Service (RUS) which offers telecommunications and electric programs along with water and sewer programs; the Rural Housing Service (RHS) which includes rural housing programs as well as rural community loan programs; and, the Rural Business-Cooperative Service (RBCS) which includes cooperative development and technical assistance, plus other business development programs.

2.4.4 *Food, Nutrition, and Consumer Services*

The mission of Food, Nutrition and Consumer Services (FNCS) is to ensure access to nutritious, healthful diets for all Americans. Through food assistance and nutrition education for consumers, FNCS encourages consumers to make healthful food choices. Today, rather than simply providing food, FNCS works to empower consumers with knowledge of the link between diet and health, providing dietary guidance based on research.

The Food, Nutrition and Consumer Services Mission Area is organized into two areas: The Food and Nutrition Service (FNS) and the Center for Nutrition Policy and Promotion.

2.4.5 *Food Safety*

Assuring that the nation's meat and poultry supply is safe, wholesome, unadulterated, and properly labeled and packaged is the mission and responsibility of the Food Safety mission area.

The Food Safety and Inspection Service (FSIS) conducts specific activities to ensure the safety of meat and poultry products.

2.4.6 *Research, Education, and Economics*

The Research, Education and Economics mission area strives to develop cutting edge technologies that improve food and fiber production and enhance the safety of the national food supply. USDA research finds many new uses for the nation's agricultural bounty, improves crop varieties and prevents crop losses and animal diseases caused by various pests and pathogens.

The Research, Education and Economics mission area also provides economic and statistical information and analysis for public and private sector decisions on agriculture, international trade, food, natural resources and rural America..

The Research, Education and Economics mission area is organized into four agencies; the Agricultural Research Service, the Cooperative State Research, Education, and Extension Service, the Economic Research Service and the National Agricultural Statistics Service.

2.4.7 Marketing and Regulatory Programs

The mission of Marketing and Regulatory Programs mission area is to facilitate the domestic and international marketing of U.S. agricultural products and to ensure the health and care of animals and plants while improving market competitiveness and the economy for the overall benefit of both consumers and American agriculture.

The Marketing and Regulatory Programs mission area is organized into three Agencies: Agricultural Marketing Service, Animal and Plant Health Inspection Service, and Grain Inspection, Packers and Stockyards Administration.

2.4.8 Other Departmental Organizations

The other Departmental Organizations provide central administrative services and policy support to USDA agencies. They include:

- Departmental Administration which includes; the Board of Contract Appeals, the Office of Administrative Law Judges, the Office of Administrative Support, the Office of Civil Rights, the Office of Human Resources Management, the Office of Judicial Officer, the Office of Operations, the Office of Outreach, the Office of Procurement and Property Management, and the Office of Small and Disadvantaged Business Utilization.
- Office of the Chief Financial Officer
- Office of the Chief Information Officer
- Office of Communications
- Office of Congressional Relations
- Office of Budget and Program Analysis
- Office of Chief Economist
- Office of Executive Secretariat
- Office of Inspector General
- National Appeals Division

- Office of General Counsel

2.5 Dependencies

Given full Year 2000 compliance of USDA’s core processes and key support processes, the Department must still rely on the compliance of other Federal, State and local agencies and the private sector. All commercial-off-the-shelf software must be certified Year 2000 compliant, and data exchanges outside the Department must be compliant.

For example, the U.S. Treasury, Federal Reserve and Automated Clearing House (ACH) are responsible for making all of the government employee payroll each month by printed check and electronic funds transfer. The large employers that submit wage reports electronically or on magnetic media must use software and systems that are Year 2000 compliant to generate the data. The same is true for the States that provide vital statistical information and the other government agencies that regularly exchange data with USDA.

In addition, the number of common devices that have an impact on day-to-day operations is enormous. These devices rely on embedded chips that may or may not be affected by the year 2000 change. Some of these are as basic as the chip that controls a traffic light, or as complicated as a computer-based system that controls the heating, ventilation and power in an office building or research laboratory.

Public utilities are also vital to continued operations. These include electrical power that feeds all USDA facilities, and telephone lines, which are basic to providing voice and data communication services. Year 2000 compliance of these utilities is no less important than the Year 2000 compliance of USDA’s internal systems.

3.0 The Planning Process

Business Continuity Planning is the ongoing process of creating, testing, and maintaining the policies and procedures to ensure that service and program delivery are not compromised because of the year 2000 problem.

It is essential that business continuity (contingency) planning begins immediately. All Agencies must reduce the risk and potential impact of year 2000-induced information system failures of their core business processes by implementing rigorous business continuity planning processes.

The planning process gives a structured approach to aid the Mission Area and Department Administration executive management team in business continuity and contingency planning. The process draws on the work of leading organizations in the information technology industry and incorporates their guidance and practices. Many of the Year 2000-related concepts and practices presented in this planning process build upon existing best practices in the contingency and disaster recovery areas.

The planning process consists of five phases--supported by Mission Area Year 2000 program management. Each phase represents a major Year 2000 business continuity planning project activity or segment.

3.1 Business Continuity (Contingency) Plan Development

The BCP is developed in a logical, stepwise process in five phases. The process begins in the *Initiation Phase* by first obtaining management support to assign staff to a work group. The next step is to *Analyze* the agency's mission *and Define* the core business processes. Then we perform a *Risk and Impact Assessment* to determine the extent of risk or exposure the Year 2000 computer problem may have on our mission-critical operations. After assessing the impact we can begin to complete our *Contingency Planning* by developing a solution to the risk or risks posed. The key thing to remember here is that we must develop a plan that will insure continuous business operations with minimal disruptions. In the last phase, Validation Testing, we seek to prove that the contingency plan, developed in the previous phase, does in fact allow us to continue business operations, even if at a reduced level, until the automated systems are back in service. This process is described in some detail in the following sections.

3.1.1 Initiation—PHASE I

Initiation

The plan starts with executive level support from the Assistant or Under Secretary and Agency Heads in terms of resource allocation and personal involvement. A Senior Executive is assigned responsibility and begins by organizing a work group team within each agency. The work group begins by developing a high-level business continuity planning strategy consistent with each Mission Area core business processes.

The strategy conveys the essential core functions that must be performed. After identifying the essential business core functions that must be performed to stay in business the work group develops a master schedule and sets milestones that must be met in order to complete the BCP. Specific time tables must be based on the appropriate event horizon (see 3.2.3), which is defined as the date when any disruption to continuous operations is realized as a result of the Year 2000 date problem.

Executive management needs to be fully aware of the potentially devastating financial, organizational, and political consequences of the failure of one or more mission-critical information systems. Agency executives must dedicate sufficient resources and staff for the business continuity planning tasks, and ensure that senior managers support this effort to develop the plan, the following steps must be implemented:

Step 1: Establish a business continuity project work group.

Within the Mission Area, establish a business continuity work group. The group should include representatives from the Mission Area's major business units, domain experts in relevant functional areas, business continuity and disaster recovery specialists, program analysts, and contract specialists. Access to legal advice is also a necessity. This group should work closely with the OCIO Year 2000 Executive Director and staff to ensure access to information on the status of the Mission Area's Year 2000 renovation, validation, and implementation efforts.

Step 2: Develop and document a high-level business continuity planning strategy

A high-level business continuity planning strategy provides the Mission Area's executive management with an overview of the year 2000 business risks and solutions. The strategy should address the project structure, its relationship with the Year 2000 program, metrics and reporting requirements, and the initial cost and schedule estimates. The risk of business failure is not limited to the organization's internal information systems. Many USDA agencies also depend on information and data provided by their business partners—including other federal agencies, hundreds of state and local agencies, international organizations, and private sector entities. Finally, every organization also depends on services provided by the public infrastructure—including power, water, transportation, and voice and data telecommunications.

Step 3: Identify core business processes

Agencies should analyze existing business plans and work with business process owners, the OCIO, and Year 2000 program staff to identify core business processes and supporting mission-critical systems for each business area. This information should be documented and mapped to the core business process of the Agency and the Mission Area (see chart **Appendix C**).

This step ensures that all key business dependencies are clearly identified, including infrastructure and external sources of critical supplies and information.

Step 4: Define roles and assign responsibilities

Define roles and assign responsibilities for leading the planning effort and for performing analyses and designing business alternatives, including contingent operations for sustained and prolonged disruption. Appoint individuals to lead the development of contingency plans for each of the core business processes. Define responsibilities for documenting the business continuity plan and defining the essential operational activities comprising it. Ensure those individuals responsible for the various business continuity and contingency planning activities are held accountable for the successful completion of individual tasks. The core business process owners are responsible and accountable for meeting the milestones for the development and testing of contingency plans for their core business processes.

Step 5: Develop a master schedule and milestones

Develop a schedule for the planning effort and the delivery of interim and final products. Link the schedule to critical stages in the Year 2000 program effort. Update as required.

Step 6: Implement a risk management process and establish reporting system

Manage the business continuity planning tasks and activities as a sub-project within the Year 2000 program office. Rank business risks and focus the planning effort on the greatest risk to critical core business processes. Identify project risks and develop metrics. Establish reporting system, reporting requirements, and formats. Track estimates and after each step is completed update estimates as needed, especially when new information significantly alters the estimates. Estimate and assign risk to each mission-critical system undergoing renovation or replacement. Track and compare actual costs against estimates.

Step 7: Assess existing business continuity, contingency, and disaster recovery plans and capabilities

Assess existing business continuity, contingency, and disaster recovery plans for their applicability. Identify weaknesses and strengths of existing plans. Upon completion of the assessment make the necessary changes or modifications to account for the weaknesses.

Step 8: Implement independent reviews

Task the Mission Area and Agency's quality assurance staffs to review the business continuity planning processes. For example, use the quality assurance office staff to ensure that the business continuity team reviews existing contingency plans and that the existing contingency and disaster recovery plans are updated and incorporated into the business continuity plan. The quality assurance reviews should examine the worst case scenarios to ensure that a feasible backup strategy--including private sector solutions--can be successfully implemented in a national emergency.

3.1.2 Analysis and Definition—PHASE II

Analysis & Definition

After setting milestones and developing an approved master schedule the next phase is to begin defining the essential business functions that must be performed to continue providing the expected service. The work group then assesses the potential impact of each mission-critical systems failure of the Agency's core business processes and functions.

Step 1: Define and document information requirements, methods, and techniques to be used in developing the business continuity plan

Define the information requirements for constructing a business continuity plan. These requirements generally fall into four categories: (1) business process composition, execution cycles, and support; (2) operational priorities, service levels, dependencies, and relationships; (3) the primary and collateral Year 2000 business risks and the business scope of their impact; (4) and, the costs and benefits of business continuity strategies and alternatives. Each area has detailed information requirements that are essential to providing effective business continuity. For example, the analysis of business process support should provide information on the technical, functional, organizational, and infrastructure support requirements. When collected, analyzed, and synthesized, the information defines a model of critical processes and risks to the business.

Step 2: Define and document Year 2000 failure scenarios

Assess business vulnerabilities and their impacts and define the Year 2000 risk scenarios. Assume the loss of all mission-critical information systems due to post-implementation failures or delays in renovation and testing.

Consider the possibility that Year 2000 date problems may be encountered earlier than expected, and address the potential disruption of essential infrastructure services, including electric power, telecommunications, and transportation.

3.1.3 *Risk and Impact Assessment – PHASE III*

Risk & Impact Assessment

All risks must be evaluated against an established standard process or procedure based on the current business operational environment. The risk and impact assessment requires a complete analysis of all business processes. However, not all business processes are equal and as a result you will prioritize them based on their importance in accomplishing each Agency's mission.

Step 1: Perform risk and impact analyses of each core business process

Monitor the status and progress of the Year 2000 program and review and verify risk metrics and critical milestones for all mission-critical systems undergoing renovation or replacement. Evaluate Year 2000-related risks posed by customers, suppliers, information technology vendors, and business partners.

Determine the impact of internal and external information system failures and infrastructure services on each core business process. Consider acquiring business impact analysis tools such as IT Thinking Tools, StarBase, etc. These tools will provide consistent analytical structure and processes, and help to standardize the impact analyses throughout the enterprise. For the core business processes and supporting business areas, analyze both manual and automated functional requirements, manual and automated system support requirements, infrastructure support requirements, suppliers, customers, service levels, processing cycles, and the external and internal business drivers. Identify critical functions, recovery priorities and timing, and dependencies to other systems and processes.

If a core business process receives data from an external organization, contact that organization and obtain the status of its Year 2000 remediation effort. If there are reasons to be concerned, address these concerns in contingency plans. Estimate the potential cost of service disruptions. In estimating impacts, address the duration of each disruption. Consider using a scorecard to aggregate and track the risk and impact information.

Step 2: Assess and document infrastructure risks

Monitor the Year 2000 readiness of the public infrastructure, including power and telecommunications services. Assess the risk of service outages, and the potential impact of outages on the core business processes. Review current contingency and disaster recovery plans to determine whether emergency services may be available to mitigate outages.

Step 3: Define the minimum acceptable level of outputs and services for each core business process

For each core business process, define the minimum acceptable level of output and the recovery time objective.

3.1.4 Contingency Planning – PHASE IV

Contingency Planning

Contingency planning integrates and acts on the results of business impact analysis. The output of this process is a business continuity plan consisting of a set of contingency plans--with a single plan for each core business process and infrastructure component. Each plan should provide a description of the resources, staff roles, procedures, and timetables needed for its implementation.

Step 1: Assess the cost and benefits of identified alternatives and select the best contingency strategy for each core business process

Assess benefits, costs, and risks of alternative contingency strategies. Select a strategy that is practical, cost-effective, and appropriate to the organization. In addition, the alternatives and strategies should provide a high level of confidence in recovery capability.

Three important factors in the selection process are:

- ✓ functionality: the degree to which the replacement functionality supports the production of a minimum acceptable level of output for a given core business process,
- ✓ deployment schedule: the time needed to acquire, test, and implement, and
- ✓ cost: life cycle cost, including acquisition, testing, training, and maintenance.

The goal is to maximize the functionality and speed of business resumption.

Step 2: Identify and document contingency plans and implementation modes

Develop a contingency plan including strategies capable of meeting minimum acceptable output requirements for each core business process. Consider the following strategies:

- ✓ quick fix,

- ✓ partial replacement,
- ✓ full redundancy or replacement, and
- ✓ outsourcing to the private sector.

Consider three basic implementation modes for the quick fix, partial, and full replacement of functionality provided by failed mission-critical systems:

- ✓ manual replacement,
- ✓ semi-automated replacement, and
- ✓ automated replacement.

A manual alternative normally requires hiring and training of additional staff. It can be used to replace all or part of a failed automated process. A semi-automated alternative can implement “bare bones” functionality, using a combination of compliant off-the-shelf applications, such as accounting software or standard database products. Some core business processes may be fully supported by compliant off-the-shelf application packages that can be purchased and rapidly installed. However, even projects that rely on off-the-shelf replacement packages may fall behind schedules. Finally, redundant business services may be provided through outsourcing contracts.

Step 3: Define and document triggers for activating contingency plans

Once the business continuity planning team selects the best contingency alternative for each core business process, it must then define triggers that would implement each plan. The information needed to define the implementation triggers for contingency plans is derived from two key sources:

- ✓ the deployment schedule for each contingency plan and
- ✓ the implementation schedule for the renovated or replaced mission-critical systems.

The deployment schedule establishes the date at which the contingency plan must be implemented if is to be to be fully tested before December 31, 1999. For example, if the contingency plan calls for an 8-month deployment schedule, the tentative implementation date should be set for April 30, 1999.

Step 4: Establish a business resumption team for each core business process

Work with core business process owners to establish business resumption teams. These teams would be responsible for managing the implementation of contingency plans and would deal with a wide range of operational problems, including the potential failures of systems thought to be renovated and tested, and the potential failures of external systems and data exchanges.

Step 5: Develop and document "zero day" strategy and procedures

Develop a risk-reduction strategy and procedures for the period between Thursday, December 30, 1999, and Saturday, January 1, 2000. This strategy may include an Agency-wide shutdown of all of its information systems on Friday, December 31, 1999, and a phased power-up on Saturday, January 1, 2000. The agency may consider extending the shutdown to infrastructure systems, including local area networks, elevators, and building management systems.

3.1.5 Validation Testing – PHASE V

Validation Testing

The objective of business continuity testing is to evaluate whether individual contingency plans are capable of providing the desired level of support to the Mission Area's core business processes and whether the plans can be implemented within a specified time period. In instances where a full-scale test may be too costly, the agency may consider end-to-end testing of key contingency plan components. An independent audit of the plan can validate the soundness of the proposed contingency strategy. Similarly, a legal review can provide assurance that the plans comply with government regulations and that liabilities and exposures are being adequately addressed.

Step 1: Validate business continuity strategy

Develop and implement a strategy for validating the business continuity plan within the time that remains. A typical strategy defines a minimum number of individual and joint exercises that combine training with testing. There are several common techniques that can be employed, including reviews, rehearsals, and quality assurance audits.

Step 2: Develop and document contingency test plans

Define and document the contingency test plans. Review the test plans and make needed changes. Ensure that management approves the plans. Disseminate the documents, provide guidance, and establish a help desk. Test plans should address the following:

- ✓ test objectives,
- ✓ test approach,
- ✓ required equipment and resources,
- ✓ necessary personnel,
- ✓ schedules and locations,
- ✓ test procedures, and
- ✓ expected results and exit criteria.

Step 3: Establish test teams and acquire contingency resources

Establish test teams responsible for preparing and executing the contingency plan tests. Test preparation may include leasing a test facility and hiring and training needed staff.

Step 4: Prepare for and execute tests

Assign responsibilities to test team members, including executives, observers, and contractors.

Step 5: Validate the capability of contingency plans

Validate the functional capability of each contingency plan. Examine test results for accuracy and consistency and note discrepancies. For each contingency plan, ensure that:

- ✓ There is adequate capability to manage, record, and track the contingency transactions through the alternative business process;
- ✓ The manual activities in particular, and the alternative business process in general, meet an acceptable level of performance;
- ✓ An acceptable level of quality control is provided to critical parts of the alternative business process, and an acceptable level of integrity and consistency is provided to alternative databases;
- ✓ An acceptable level of security is provided to the data captured by an alternative data capture mechanism;
- ✓ Contingency database requirements have been defined for alternative implementation modes, and contingency bridges can provide conversion from the contingency environment back to the "normal" production environment; and
- ✓ Any functional differences between the normal business process and the alternative business process can be reconciled or adjusted at the database level.

Step 6: Rehearse business resumption teams

Rehearse business resumption teams to ensure that each team and team member is familiar with business resumption procedures and their roles.

Step 7: Update the business continuity plan based upon lessons learned and re-test if necessary

Resolve shortcomings and problems noted during testing and update each continuity plan. When under time constraints, prioritize the problem areas. For example, procedural problems involving internal administrative functions are not as serious as technical problems directly affecting the resumption of operations. Ongoing changes in systems, software, applications, communication, and operations will also require updates to the plan. A re-test may be required to ensure that the problems do not recur and that the updated plan does provide the specified capability.

Step 8: Update disaster recovery plans and procedures

Update disaster recovery plans. Ensure that all newly developed or acquired contingency applications and other software components are included in the disaster recovery update cycle.

3.2 Business Continuity (Contingency) Plan Matrices

The completed BCP will consist of this document and each completed Mission Area matrix included as an appendix. The following instructions are keyed to the sample matrix template in ***Appendix B***.

3.2.1 Section Number

This is self-explanatory. Number each risk or threat sequentially beginning with the root number of your Mission Area.

3.2.2 Risk/Threat

List with sufficient detail the specific risk or threat that occurs to prevent the core business function developed in the identification phase from being performed. Underline the specific risk and follow it up with a brief description of which related systems or processes are also affected, or that may be the cause of the problem. (Example: NFC is unable to post earnings (W-2s), make corrections to Earnings records, or access earnings data due to Year 2000 related problems with automated systems. Earning processes are supported by automated systems such as Annual Wage reporting (AWR), Detailed Earnings Query (DEQ), Summary Earnings Query (SEQ), and Employer Earnings System (EES). Interfacing systems are: Individual Income and Wage Reporting (IIWR), Treasury and Summary Employee Earnings Statement (SEES) Social Security Administration.)

3.2.3 Event Horizon (Time To Failure)

Enter the date when this risk will occur based on the analysis i.e., the date when the core business process would not operate because of a Year 2000 related problem. The first working day in the Year 2000 is January 3rd, which is the default Event Horizon. However, where a replacement strategy is being used to become Year 2000 compliant or the processing does forward calculations using dates calculated in the future this could be considerably sooner. (Example: Telecommunications hardware. If an organization desired to replace the entire suite of hardware including routers, switches and servers with Year 2000 compliant equipment the manufacturing, shipping, installation, and testing time must be calculated for each of these components to determine the longest lead time required. Missing that date in ordering the replacement hardware would mean the solution could not be accomplished prior to January 3, 2000.) Be sure to allow plenty of time for testing in all cases. When implementing testing and the Business Continuity Plan, the following failure horizon dates should be monitored:

Potential Horizon Failure Dates	
Failure Date	Testing Purpose
January 1, 1999	To ensure that the digits ?999? do not trigger a red flag, other program subroutine(s), or cause a processing error
August 22, 1999	Overflow of ?end of week? Rollover
September 9, 1999	To ensure that the digits ?99? or ?9999? do not trigger a red flag, other program subroutine(s), or cause a processing error
October 1, 1999	First day of Fiscal Year 2000
January 1, 2000	Key date in any compliance testing
January 3, 2000	First full work day in the new year
January 10, 2000	First 9 character date
February 28, 2000	To ensure the leap year is being properly accounted for
February 30, 2000	To ensure that this date is not processed
February 31, 2000	To ensure that this date is not processed
March 1, 2000	To ensure date calculations have taken leap year into account
October 10, 2000	First 10 character date
December 31, 2000	366th day of the year
January 1, 2001	First day in the 21st Century

3.2.4 Business Priority, Score

The business priority is used to determine the most mission-critical areas to which resources should be applied to prepare for a potential failure. It is represented as a numerical score; the highest number reflects the highest priority. The business priority itself was derived from two factors, the risk assessment and impact of a failure on USDA’s ability to continue to do business. The Score is achieved by multiplying the risk assessment number times the impact number.

Risk assessment is the probability that the risk or threat will occur, and is expressed numerically on a scale of 0 to 1.0. The following factors are considered in determining the risk assessment:

- Whether the system is internal or external to USDA;
- The number of external influences;
- Whether the system involved new or improved technology;
- The total number of dependent systems and processes; and,
- The status of renovation and testing.

Because factors such as the status of renovation and testing will change as time progresses, it is possible that the business priority will change as the Year 2000 nears. Risk Assessment terminology is defined by the following:

Contains Interfaces - Interfaces where data values are exchanged with other IT systems.

New or Improved Technology - Using new software (other than version upgrades) or computing platforms (e.g., use of Internet).

In Renovation – The system is currently being either replaced or repaired to make it Y2K compliant.

In Testing - The replaced or repaired system is currently being tested to verify Y2K compliance.

Fully Implemented System - The replaced or repaired system has satisfactorily completed Y2K testing and is currently operational.

Risk Assessment

Select one column and check all that apply:

		(Renovation Strategy)	
	Value	Repair	Replace
Replaced System	0.9		
Repaired Systems	0.8	X	
New or Improved Technology	0.7	X	
In Renovation	0.6	X	
In Testing	0.5		
Contains one or more External Interfaces	0.4	X	
Contains one or more Internal Interfaces	0.3	X	
Contains No Interfaces	0.2		

Risk Assessment Score: ======================> 0.56

(Total all values and divide by the number of boxes checked)

(Round to the nearest 100ths)

Impact Assessment also expresses a numeric range of values from 1 to 10. It reflects the degree of damage to USDA's ability to deliver service to its customers if the risk or threat occurs. The higher the value, the more severe the impact on service delivery. Factors contributing to determining the degree of impact are:

- The degree of effect of failure on business operations;
- The scope of the problem and the number of customers who would be affected;
- The effect on the ability to make a payment; and,
- Whether the failure would cause an immediate effect, a delayed effect, or no effect on the customer.

Impact Assessment terminology is defined as follows:

Degree of Effect on Business Operations

HIGH = Complete or nearly complete shutdown of services

MEDIUM = Significant loss of quality and/or quantity of services

LOW = Little or no impact on service

Scope of Problem

LARGE = Impact value of $1 million or more

MEDIUM = Impact value between $100,000 and $999,999

SMALL = Impact value of $999,999 or less

Note: Estimate impact value as related to health and safety, financial well being to individuals, and/or the economy

Effect on Customer

IMMEDIATE = Impact is evident to customers within 1 to 5 days of failure

DELAYED = Impact evident to customers within 6 days or longer after failure

NONE = There is no impact to customers, or the public

Impact Assessment

Select Only One in Each category That Apply:

Degree of Effect on Business Operations (High)	10	X
Degree of Effect on Business Operations (Medium)	9	
Degree of Effect on Business Operations (Low)	8	
Scope of Problem (Large)	7	X
Scope of Problem (Medium)	6	
Scope of Problem (Low)	5	
Effect on Health & Safety, Financial and Economic Impact	4	X
Effect on Customer (Immediate)	3	
Effect on Customer (Delayed)	2	X
Effect on Customer (None)	1	

Total Impact Assessment Score, (Total the Points and Divide By the number of boxes checked): 5.75

Business Priority Score:

Total Risk Score (x) Impact Score (Round to Nearest Hundredth) = 3.22

3.2.5 Risk Mitigation Strategy

The Risk Mitigation Strategy with corresponding Milestone Dates and Action Components are actions to be taken which are designed to eliminate or reduce the impact or likelihood of a risk or threat prior to the event horizon or time to failure. These are actions, which will be taken between now, and the event horizon to prevent the threat from occurring. These are drawn from the Year 2000 project management information as well as actions identified by the BCP team.

3.2.6 Milestone Dates

Enter the milestone date that the risk mitigation strategy will be completed. Enter a separate milestone date for each mitigation strategy. (Example: a) complete renovations of all Earnings software systems. Sep 1998; b) Complete forward date, integration testing of all Earnings and related systems. Dec 1998; etc.)

3.2.7 Action Agent

Enter the Agency or organization whose chief executive has responsibility for completing the associated risk mitigation strategy by the milestone date.

3.2.8 Contingency and Triggers

The Contingency and Triggers element of the matrix identifies the events that set the contingency plan in motion. Referred to be a detailed existing plan and plans under development at the local level. The described actions maximize the available functionality and trigger the activities needed to resume normal operations.

4.0 Contingency Plan Testing

The objective of business continuity testing is to evaluate whether individual contingency plans are capable of providing the desired level of support to the Department’s core business processes. Testing will also validate whether a given plan can be implemented within a specified time period, and provide an opportunity to make adjustments to the plan and the environment within which the plan is tested e.g., readiness of the facility to deliver service during a contingency. Finally, testing allows the opportunity for a detailed assessment of the cost of operating under a contingency.

Each responsible component will comprehensively test their plan or plans. While emphasis will be placed on those risks carrying the higher business impact scores, all plans will be sufficiently tested to demonstrate their ability to allow business to be conducted during a contingency.

4.1 Test Guidelines and Environment

In order to ensure their validity, each plan will be reviewed and tested within the guidelines set forth in the GAO’s February 1998 Exposure Draft, *Year 2000 Computing Crisis: Business Continuity and Contingency Planning*. These guidelines include provisions for review and rehearsal.

4.2 Review

At each stage of development, the ability to provide acceptable levels of service delivery under various systems failure scenarios should be considered. The review process should include program managers and workgroup.

On completion, plans should be reviewed by the BCP team (Agency Heads, Senior Executive Sponsors, and the Assistant or Under Secretary for each Mission Area) to see that all elements are provided. These elements include, but are not limited to, provisions for staff training, availability of supplies such as forms to be used when reverting to a manual process, availability of backup facilities, availability of procedures, and triggers for return to normal operations.

4.3 Rehearsal

There are two types of rehearsal the desktop exercise and simulation.

4.3.1 Desktop Exercise

In the desktop exercise, the manager responsible for implementing a contingency plan will be advised of a hypothetical contingency situation. The manager, or his designee, will then use the plan to work out a response to the situation. The manager will answer questions that relate to the availability of trained staff, adequacy of the facilities, adequacy of the machines, and whether forms and supplies are on hand. Adjustments will be made either to the plan or to the particular environment during this phase should any part of the plan fall short of its objective.

4.3.2 Simulation

Actual simulation takes the desktop exercise a step further. In actual simulation testing, a component or office (or part of an office) will conduct real business as if in a contingency situation. The simulation will be thorough enough to assure the component manager that on-site personnel can handle the work, the training has been carried out or scheduled, needed supplies are available, and that the facility can be adapted to the contingency. At this point, any inadequacy in the plan or the office's preparation will be remedied in advance of an actual contingency situation.

4.4 Process For Plan Updates

The BCP should be updated as needed to reflect new or changed information. The revisions will reflect plan changes that occur as a result of changes in status of mitigation efforts, review of individual plans, and needed adjustments stemming from contingency plan testing. All BCP changes and updates to the printed plan will be coordinated through the OCIO, Year 2000 Program Office.

5.0 Outreach Strategy

In developing the Business Continuity Plan each Mission Area should ensure that awareness activities are part of the document. The overall plan must include an assessment of the external interfaces of data, processes, and operating procedures. Where appropriate the BCP will identify those external interfaces that pose a risk on all mission critical systems that may potentially adversely effect the continuity of business operations.

An example of the types of activities required to develop this information is available in the USDA Chief Information Officer's testimony before the Senate Committee on Agriculture, Nutrition and Forestry. The USDA CIO stated that she had requested assistance of the Under Secertaries for Farm and Foreign Agriculture Services and Research, Education and Economics in developing an assessment of the effects of Year 2000 on production agriculture.

The USDA assessment will cover two aspects; 1) an analysis of the equipment and systems affected at the farm level, and 2) an assessment of the potential economic affect when factoring in all of the aspects involved in getting a product to market (transportation, processing, food distribution, retail). This information will be invaluable for these Agencies to use in assessing the impact to business continuity.

It is essential for all Agencies to assess the impact of the Year 2000 on their customers and stakeholders and determine in a like manner the effect of that impact on their core business areas. Then steps should be taken to include a risk mitigation strategy in the BCP for resolution of that risk. Of course, as part of the outreach strategy this information should be shared with the customer or stakeholder to increase the probability that all Year 2000 impacts are minimized.

6.0 Mission Area and Departmental Organizations BCP Matrices

Each Mission Area BCP will become a part of the Department BCP. Copies of all approved plans will be maintained on file in the OCIO Year 2000 Program Office. The manner of their development is described in section 2.1, *Business Continuity (Contingency) Plan Development* above.

APPENDIX A

GLOSSARY

The definitions in this glossary were developed by the project staff or were drawn from other sources, including the *Computer Dictionary*: *The Comprehensive Standard For Business*, *School*, *Library*, and *Home*, *Microsoft Press*, Washington, D.C., 1991; *The Year 2000 Resource Book*, *Management Support* Technology Corp., Framingham, Massachusetts, 1996; *The Year 2000 and 2-Digit Dates: A Guide for Planning and Implementation*, International Business Machines Corporation, 1997; *Denis Howe's "Free On-line Dictionary of Computing*,"; and the Gartner Group's "*IT Glossary*".

Application

A computer program designed to help people perform a certain type of work. Depending on the work for which it was designed, an application can manipulate text, numbers, graphics, or a combination of these elements.

Architecture

A description of all functional activities to be performed to achieve the desired mission, the system elements needed to perform the functions, and the designation of performance levels of those system elements. An architecture also includes information on the technologies, interfaces, and location of functions and is considered an evolving description of an approach to achieving a desired mission.

Business Area

A grouping of business functions and processes focused on the production of specific outputs.

Business Architecture

A description of the systems, databases, and interactions between systems and databases that will be needed to fulfill business requirements.

Business Continuity

The sum of an organization's businesses. It includes all of the core business functions, which define the organization.

Business Continuity Plan

In the context of the Year-2000 program, the overall plan, including risk mitigation strategy, contingencies, and recovery, to ensure the organization's core business processes continue in spite of disruptions to infrastructure and/or support systems.

Business Function

A group of logically related tasks that are performed together to accomplish an objective.

Business Plan

An action plan that the enterprise will follow on a short-term and/or long-term basis. It specifies the strategic and tactical objectives of the enterprise over a period of time. The plan, therefore, will change over time. Although a business plan is usually written in a style unique to a specific enterprise, it should concisely describe "what" is planned, "why" it is planned, "when" it will be implemented, by "who" it will be implemented, and "how" it will be assessed. The architects of the plan are typically the principals of the enterprise.

Business Priority

A score derived by multiplying Risk Assessment and Impact ranging from 0 (low) to 10 (high). The score can help the organization determine areas of emphasis and where resources will be employed when it becomes obvious not all risks/threats can be mitigated.

Contingency

Planned action(s) to eliminate or reduce the Impact of a risk/threat at or after the Time Horizon to Failure.

Contingency Plan

In the context of the Year 2000 program, a plan for responding to the loss or degradation of essential services due to a Year 2000 problem in an automated system. In general, a contingency plan describes the steps the enterprise would take including the activation of manual or contract processes to ensure the continuity of its core business processes in the event of a Year 2000-induced system failure.

Core Business Process

A grouping of business related events or functions that define the central business operations in terms of producing a desired result.

Day 1 Strategy

A risk-reduction strategy and procedures for the period between mid-November 1999 and mid-January 2000 that will be documented in a detailed Day 1 Plan.

Impact

The degree of effect on a whole number scale of zero (low) to 10 (high) that a risk/threat will have on the organization if it is not mitigated.

Infrastructure

The facilities, equipment, installations, and support systems needed for the functioning of a system.

Interface

A boundary across which two systems communicate. An interface might be a hardware connector used to link to other devices, or it might be a convention used to allow communication between two software systems.

Magnetic Media

Tape, cartridges and floppy disks used for storing data.

Metrics

Measures by which processes, resources, and products can be assessed.

Mission-critical system

A system supporting a core business activity or process.

Portfolio

In the context of the Year 2000 program, an inventory – preferably automated – of an agency's information systems and their components grouped by business areas.

Quality Assurance

All the planned and systematic actions necessary to provide adequate confidence that a product or service will satisfy given requirements for quality.

Risk Assessment

An activity performed to identify risks and estimate their probability and the impact of their occurrence; it is used during system development to provide an estimate of damage, loss, or harm that could result from a failure to successfully develop individual system components.

Risk Management

A management approach designed to prevent and reduce risks, including system development risks, and lessen the impact of their occurrence.

Risk Mitigation

Action(s) taken to eliminate or reduce the Impact or Likelihood of a risk/threat prior to the Time Horizon to Failure.

Risk/Threat

Event or non-event having a negative impact on or endangering a core business function or critical system of the organization.

Strategic Plan

A long-term, high-level plan that identifies broad business goals and provides a roadmap for their achievement.

System

A collection of components that support core business processes or activities and enable product, program or service delivery.

System Infrastructure

The computer and communication hardware, software, databases, people, and policies supporting the enterprise's information management functions.

Test

The process of exercising a product to identify differences between the expected and actual behavior.

Test Facility

A computer system isolated from the production environment dedicated to the testing and validation of applications and system components.

Time Horizon to Failure

Date when the risk/threat will first have impact.

Trigger

The event or events that cause a contingency plan to be implemented.

Validation

The process of evaluating a system or component during or at the end of the development process to determine whether it satisfies specified requirements.

“ ... with respect to information technology, …

Year-2000 Compliant

the information technology accurately processes date/time data (including, but not limited to, calculating, comparing, and sequencing) from, into, and between the twentieth and twenty-first centuries, and the years 1999 and 2000 and leap year calculations, to the extent that other information technology, used in combination with the information technology being acquired, properly exchanges date/time data with it" (48 CFR Part 39.002)

Year 2000 problem

The potential problems that might be encountered by computer hardware, software, or firmware in processing year-date data for years beyond 2000.

APPENDIX B

5.1 Core Business Process: National Finance Center, Earnings Posting

No	Risk/Threat	Event Horizon (Time to Failure)	Business Priority			Risk Mitigation Strategy			Contingency and Triggers
			Risk Assessment	Impact	Score	Mitigation Strategy	Milestone Dates	Action Agent	
5.1.1	National Finance Center (NFC) is unable to post earnings (W-2s), make corrections to Earnings records, or access earnings data due to Year 2000 related problems with automated systems. Earning processes are supported by automated systems such as Annual Wage reporting (AWR), Detailed Earnings Query (DEQ), Summary Earnings Query (SEQ), and Employer Earnings System (EES). Interfacing systems are: Individual Income and Wage Reporting (IIWR), Treasury and Summary Employee Earnings Statement (SEES) Social Security Administration.	Jan 3, 2000	.2	10	**2.0**	a) Complete renovation of all Earnings software and related systems. b) Complete forward date, system and integration testing of all Earnings and related systems. c) Develop local Year 2000 contingency plan. d) Provide refresher training on related forms processing. e) Develop plans to hire and train on contingency basis administrative staff from local area. f) Establish the Business Resumption Team for the Earnings process	Oct 1998 Jan 1999 Feb 1999 Mar 1999 Mar 1999 Mar 1999	NRS NRS NFC NFC NRS NFC	1) In the event that PRS and other systems are unable to provide automated support to the Earnings process due to critical Year 2000 date problems, the Business Resumption Team for the Earnings Process will analyze the problem, make corrections and retest immediately. 2) Automated processing of Earnings system will be suspended until corrections are made. 3) Operations components will implement the NFC Year 2000 Contingency Plan.
5.1.2									
5.1.3									

Appendix C

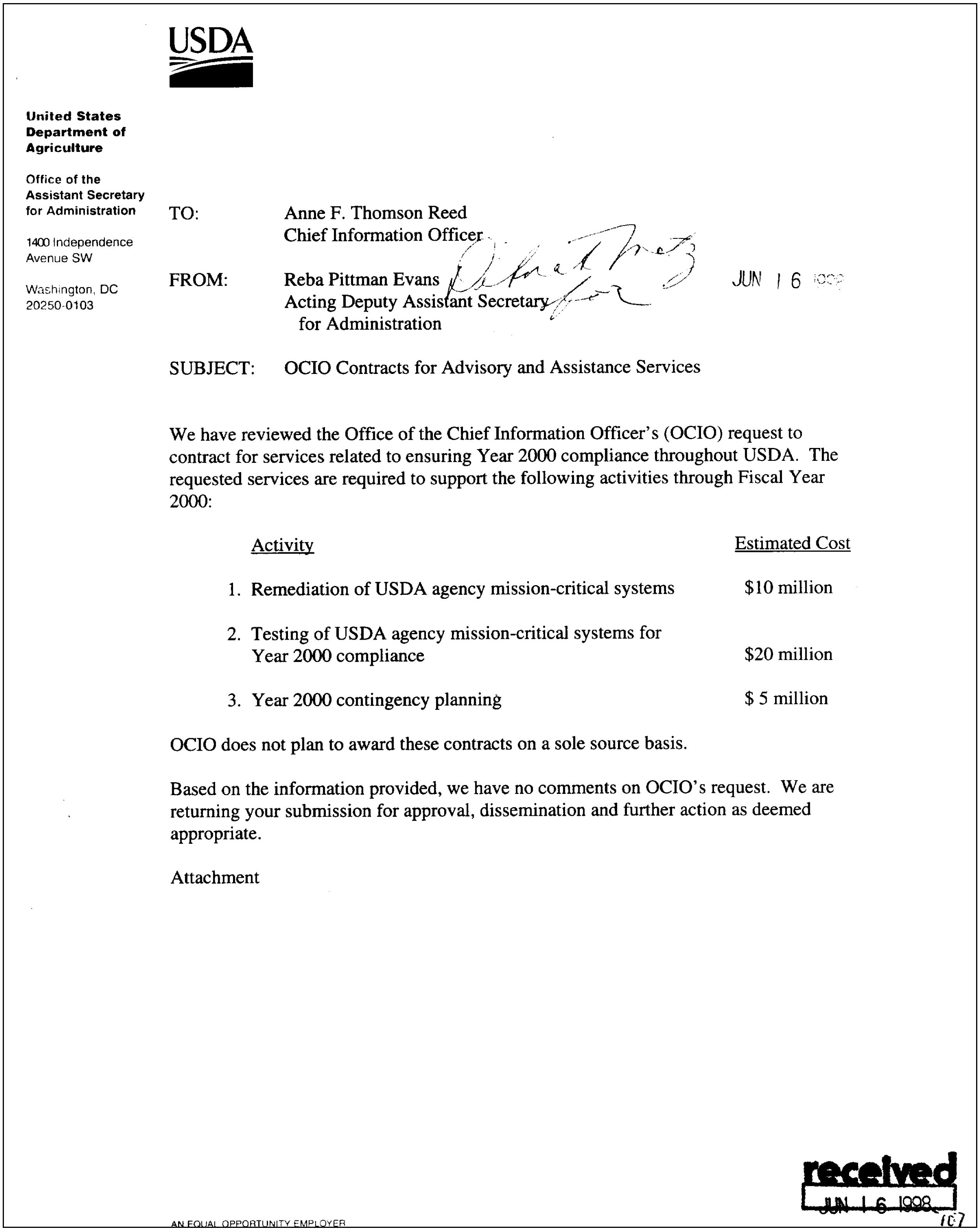
Mission Area to Core Business Process Mapping

Mission Area: Office of the Chief Financial Officer					
Agency: National Finance Center					
Core Business Process: Earnings Posting Input					
No.	**IT Systems Name**	**No.**	**Telecom Systems Name**	**No.**	**Vulnerable Systems Name**
1	Earnings Posting Audit	1	BCN Wide Area Network	1	Carrier AC Unit B2300 (1)
2	Annual Wage Reporting	2	Frame Relay S324	2	Carrier AC Unit B2300 (2)
3	Detailed Earnings Query	3	ECTN Switch	3	Carrier AC Unit B2300 (3)
4	Employer Earnings System			4	Emmerson Security System
				5	ECBL Fire and Alarm
				6	OTIS R3700 Elevator Actuator
				7	Imprint Process Controller

Mission Area: Office of the Chief Financial Officer					
Agency: National Finance Center					
Core Business Process: Earnings Posting Audit					
No.	**IT Systems Name**	**No.**	**Telecom Systems Name**	**No.**	**Vulnerable Systems Name**
1		1		1	
2		2		2	
3		3		3	
4				4	
5				5	
6				6	
7				7	
8					
9					
10					
11					

Mission Area: Office of the Chief Financial Officer					
Agency: National Finance Center					
Core Business Process: External Interfaces					
No.	**IT Systems Name**	**No.**	**Telecom Systems Name**	**No.**	**Vulnerable Systems Name**
1	Individual Income and Wage Reporting	1	None	1	None
2	Summary Employee Earnings Statement				

Appendix D



USDA

United States Department of Agriculture

Office of the Assistant Secretary for Administration

1400 Independence
Avenue SW

Washington, DC
20250-0103

TO: Anne F. Thomson Reed
Chief Information Officer

FROM: Reba Pittman Evans
Acting Deputy Assistant Secretary
for Administration

JUN 16 1998

SUBJECT: OCIO Contracts for Advisory and Assistance Services

We have reviewed the Office of the Chief Information Officer's (OCIO) request to contract for services related to ensuring Year 2000 compliance throughout USDA. The requested services are required to support the following activities through Fiscal Year 2000:

Activity	Estimated Cost
1. Remediation of USDA agency mission-critical systems	$10 million
2. Testing of USDA agency mission-critical systems for Year 2000 compliance	$20 million
3. Year 2000 contingency planning	$ 5 million

OCIO does not plan to award these contracts on a sole source basis.

Based on the information provided, we have no comments on OCIO's request. We are returning your submission for approval, dissemination and further action as deemed appropriate.

Attachment

107